Brandenburgische
Technische Universität
Cottbus - Senftenberg

08/2023 **Amtliches Mitteilungsblatt der BTU Cottbus–Senftenberg** **27.06.2023**

I n h a l t

Herausgeber: Brandenburgische Technische Universität Cottbus - Senftenberg, Präsidentin
Redaktion: Abteilung Lehre und Studium, Referat Qualitätsmanagement Studium und Lehre
Druck: BTU Cottbus - Senftenberg
Auflage: 10
https://doi.org/10.26127/BTUOpen-6351

Leitlinie zur Informationssicherheit an der Brandenburgischen Technischen Universität Cottbus–Senftenberg

Inhalt

1. Stellenwert der Informationsverarbeitung

Der mit Hilfe geeigneter Informations- und Kommunikationstechnologien durchgeführten Verarbeitung von Informationen kommt an Universitäten eine zentrale Rolle bei der Erfüllung ihrer Aufgaben zu. Die Funktionsfähigkeit der Brandenburgischen Technischen Universität Cottbus-Senftenberg (BTU) bei der Wahrnehmung ihrer Aufgaben in Studium und Lehre, Forschung und Transfer sowie in der Administration hängt ganz wesentlich von der Vertraulichkeit, Integrität und Verfügbarkeit ihrer IT-Infrastruktur ab.

Alle Bereiche der BTU verarbeiten in ihren Prozessen, Verfahren oder Abläufen Informationen. Die Universitätsleitung erkennt, dass sich die Risiken und die zu erwartenden Auswirkungen bei der Informationsverarbeitung verändern und im schlimmsten Fall für die Hochschule eine existenzielle Bedrohung darstellen können.

Um allen Angehörigen der BTU eine sichere und verlässliche Arbeitsumgebung zur Verfügung stellen zu können, ist das Ergreifen geeigneter Sicherheitsmaßnahmen sowie ein auf die ganze Universität bezogenes Informationssicherheitsmanagement von höchster Priorität. Mit der vorliegenden Amtlichen Mitteilung unterstreicht die Hochschulleitung die Bedeutung der Informationssicherheit für die Universität.

Die Leitlinie bildet die Grundlage für das Informationssicherheitskonzept der BTU. Sie beschreibt die allgemeinen Grundsätze, Ziele und Sicherheitsmaßnahmen, die für die Initiierung, Etablierung und Aufrechterhaltung eines ganzheitlichen Informationssicherheitsprozesses an der BTU erforderlich sind.

2. Grundsätze und Ziele der Informationssicherheit

Ziel der Informationssicherheit ist es, die Risiken, die auf die folgenden drei Grundwerte einwirken, auf ein vertretbares Maß zu reduzieren. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen.

Die Grundwerte der Informationssicherheit lauten:

Vertraulichkeit: Vertrauliche Informationen[1] sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Zu den Schutzobjekten gehören die gespeicherten oder transportierten Daten und Nachrichteninhalte und die Informationen über den Kommunikationsvorgang (Wer? Was? Wann?).

Vertraulichkeit wird an der BTU beispielsweise durch folgende Maßnahmen unterstützt:

- Nutzung zentraler Benutzerverwaltungssysteme mit zeitgemäßen Passwortpolicies,
- Bereitstellung von Verschlüsselungsmechanismen und -methoden für vertrauliche Informationen,
- Die Zutrittskontrolle zu Räumlichkeiten und der Zugang zu IT-Systemen wird durch ein durchgängiges Rechte- und Rollenkonzept geregelt,
- Betrieb und barrierearmer Zugang zu on-premise Kommunikations- und Kollaborationslösungen.

Integrität: Der Begriff der Integrität bezieht sich sowohl auf Informationen als auch auf IT-Systeme. Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Vollständigkeit bedeutet, dass alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben. In Bezug auf IT-Systeme bezeichnet die Integrität die vollständige und unveränderte Funktionsweise der Systeme.

Integrität wird an der BTU beispielsweise durch folgende Maßnahmen unterstützt:

- Verschlüsselung der Kommunikation zwischen Systemen,
- tägliche Sicherung der Nutzerdaten,

- Transaktionen, die aufgrund rechtlicher Anforderungen eindeutig sein müssen, werden über Protokolle geschützt.

Verfügbarkeit: Die Informationen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netze können von den Anwendern stets wie vorgesehen genutzt werden, d. h. diese müssen zu jeder Zeit einer autorisierten Person zugänglich und für diese verfügbar sein.

Die Verfügbarkeit wird an der BTU beispielsweise durch folgende Maßnahmen unterstützt:

- Systeme mit geschäftskritischen Anwendungen für Hochschulangehörige und Angebote mit Außenwirkung werden mit Hochverfügbarkeitslösungen besonders gesichert,
- die Wiederherstellung von Daten wird innerhalb von einem Tag während der regulären Betriebszeit angestrebt,
- bevorzugte Nutzung von Open Source Lösungen, um die Abhängigkeit von Dritten zu reduzieren.

Um an der BTU die Informationssicherheit zu gewährleisten, müssen jene Informationen der Universität identifiziert werden, die sie existenziell bedrohen könnten. Diese stellen die sogenannten „Kronjuwelen" der BTU dar. Ziel ist es, diejenigen Informationen der Universität zu identifizieren, die durch Bekanntwerden, Diebstahl, Zerstörung oder Kompromittierung geeignet sind, einen erheblichen Schaden zu verursachen. Als Schaden für die Universität sind sowohl Auswirkungen auf Ansehen und Reputation als auch finanzielle Folgen zu sehen.

Für die BTU sind die identifizierten „Kronjuwelen“:

- Wissen
- persönliche Daten
- Haushalts- und Finanzdaten

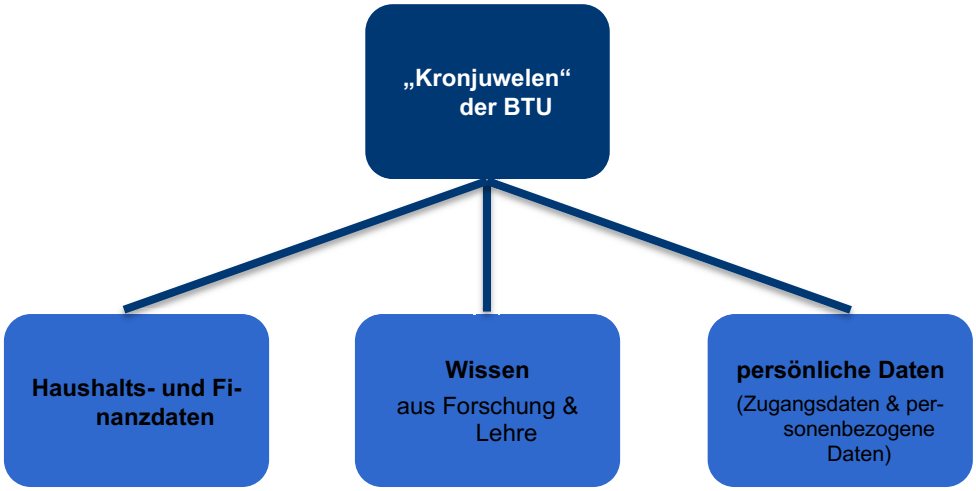

Abb. „Kronjuwelen“ der BTU

Die Bedeutung der „Kronjuwelen“ für die Universität wird nachfolgend erläutert.

Wissen aus Forschung und Lehre:

Nach dem Brandenburgischen Hochschulgesetz § 3 (1) dienen die Hochschulen „[...] der Pflege und Entwicklung der Wissenschaften und Künste durch Lehre, Forschung, Studium und Weiterbildung"[2] und sind somit für die Durchführung von Lehre und Forschung verantwortlich. Lehre und Forschung sind folglich die elementaren Kernbereiche der Hochschule. Das dort hervorgebrachte Wissen stellt somit einen Teil ihrer „Kronjuwelen“ dar.

Persönliche Daten:

Der Aspekt der persönlichen Daten setzt sich aus zwei Teilen zusammen.

Zunächst handelt es sich um Zugangsdaten, im Speziellen die Zugangskennung und das dazugehörige Passwort. Der Verlust dieser Daten stellt ein erhebliches Schadenspotenzial für die Universität dar.

Weiterhin gilt es, die personenbezogenen Daten zu schützen. Existenzbedrohend ist an diesen Informationen nicht primär der monetäre Schaden, der bei einer Datenschutzverletzung

zu erwarten ist. Viel schwerer und nicht abschätzbar sind die negativen Auswirkungen auf das Image, wenn Unzulänglichkeiten im Bereich der personenbezogenen Daten bekannt werden.

Haushalts- und Finanzdaten:

Der unberechtigte Zugang zu Haushalts- oder Finanzdaten der Universität stellt ein existenzbedrohendes Risiko dar. Insbesondere dann, wenn diese möglicherweise manipuliert werden können.

Das Primärziel der Informationssicherheit ist die Wahrung von Vertraulichkeit, Verfügbarkeit und Integrität dieser „Kronjuwelen".

Die Verfügbarkeit von Prozessen, Verfahren oder Abläufen, die die definierten „Kronjuwelen" verarbeiten, ist so zu sichern, dass kurzfristig Einschränkungen oder Beeinträchtigungen kompensiert werden können.

Fehlfunktionen und Unregelmäßigkeiten sind in Bezug auf die Integrität der Informationen und IT-Systeme nur in geringem Umfang und nur in Ausnahmefällen akzeptabel. Die Anforderungen der Informationen an die Vertraulichkeit haben ein normales, an der Gesetzeskonformität orientiertes Niveau.

Die Angehörigen der BTU gehen täglich mit großen Mengen an Informationen um. Informationssicherheit kann an der Universität daher nur etabliert werden, wenn alle Beteiligten aktiv mitwirken. Sie schützen Informationen entsprechend ihrer Werte nach bestem Wissen und Vermögen. Erklärtes Ziel ist es daher auch, alle Angehörigen der BTU im erforderlichen Umfang zu sensibilisieren und zu qualifizieren, um notwendige Kompetenzen bezüglich der Informationssicherheit aufzubauen bzw. zu vertiefen.

Die umzusetzenden Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch einen Sicherheitsvorfall erwartet wird. Zu bewerten sind dabei die Auswirkungen des Sicherheitsvorfalls auf die körperliche und seelische Unversehrtheit von Menschen, das Recht auf informationelle Selbstbestimmung, finanzielle Schäden, Beeinträchtigungen des Ansehens der Universität sowie die Folgen von Gesetzesverstößen und Beeinträchtigungen der Aufgabenerfüllung.

3. Sicherheitsmaßnahmen

Für alle Prozesse, Verfahren, Informationen, IT-Anwendungen, IT-Systeme und Räume wird der jeweilige Schutzbedarf bestimmt.

Gebäude und Räumlichkeiten werden durch angemessene Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Informationen durch ein Berechtigungskonzept geschützt.

Auf allen IT-Systemen wird, soweit technisch möglich, ein geeigneter Schutz vor Schadsoftware eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen alle Angehörigen der BTU die festgelegten Maßnahmen durch eine sicherheitsbewusste Arbeitsweise und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Die Angehörigen der BTU informieren sich durch bereitgestellte Dokumentationen und nehmen regelmäßig an Sensibilisierungs- und Schulungsmaßnahmen im Bereich der Informationssicherheit teil. Die Universitätsleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

Wenn Sicherheitsrisiken auftreten (bekannte oder drohende Angriffe), kann die Verfügbarkeit von Informationen entsprechend dem Bedrohungs- und Schadensrisiko vorübergehend eingeschränkt werden. Im Interesse der Funktionsfähigkeit der gesamten BTU ist der Schutz vor Schäden vorrangig.

Informationsverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass beeinträchtigte Prozesse oder Arbeitsabläufe kurzfristig wiederaufgenommen werden können, wenn Teile des operativen Datenbestandes verlorengehen oder offensichtlich fehlerhaft sind.

4. Informationssicherheitsmanagement

Die erfolgreiche Umsetzung der Informationssicherheit setzt klar geregelte Verantwortlichkeiten und die daraus resultierende Erfüllung von Aufgaben voraus. Zur Erreichung der Informationssicherheitsziele ist eine Sicherheitsorganisation einzurichten. Dabei sind folgende Stellen und Personen beteiligt:

Universitätsleitung

Sie ist aufgrund ihrer Gesamtverantwortung für die Risikovorsorge an der BTU auch für die Informationssicherheit verantwortlich. Die Universitätsleitung erlässt verbindliche Regeln zur Informationssicherheit für die BTU und gibt sie den Mitarbeitenden und Studierenden bekannt. Sie stellt jederzeit eine Möglichkeit zur Kenntnisnahme der aktuellen Regeln sicher. Zudem werden von der Universitätsleitung benötigte Ressourcen für die Informationssicherheit bereitgestellt.

Informationssicherheitsmanagement-Team

Die Universitätsleitung richtet ein Informationssicherheitsmanagement-Team (IS-Management-Team) ein. Aufgaben sind die Aufrechterhaltung und Fortschreibung des Informationssicherheitsprozesses sowie die Bearbeitung von Informationssicherheitsvorfällen.

Das IS-Management-Team setzt sich wie folgt zusammen:

Informationssicherheitsbeauftragte/-r (ISB):

Die Präsidentin/Der Präsident benennt eine/-n Informationssicherheitsbeauftragte/-n, die/der über eine geeignete Fachkompetenz zur Informationssicherheit verfügt. Sie/Er ist für alle operativen Belange und Fragen der Informationssicherheit der Universität zuständig und unterstützt die Hochschulleitung bei deren Aufgaben bezüglich der Informationssicherheit.

Die/Der ISB berichtet in ihrer/seiner Funktion direkt an die Präsidentin/den Präsidenten, als verantwortliche/-r Vertreter/-in der Universitätsleitung.

Mitglieder Informationssicherheitsteam

Die Mitglieder unterstützten die/den ISB bei strategischen Entscheidungen, wie z. B. der Bestimmung der Sicherheitsziele, der Sicherheitsstrategie und der Erstellung und Anpassung des Sicherheitskonzeptes. Die Mitglieder des IST sind im Informationssicherheitskonzept benannt.

Dekane, Lehrstuhlinhaber, Führungskräfte

Dekane, Lehrstuhlinhaber und Führungskräfte tragen die Verantwortung für die Informationssicherheit in ihren jeweiligen Verantwortungsbereichen und setzen die Vorgaben zur Informationssicherheit um.

Dezentrale IT-Sicherheitsbeauftragte (IT-SiBe)

Das Informationssicherheitsmanagement wird durch IT-Sicherheitsbeauftragte (IT-SiBe) unterstützt. Jede Fakultät und jede Einrichtung, die eigenständig IT-Systeme betreibt, ist verpflichtet, einen IT-SiBe zu benennen.

Informations-, Kommunikations- und Medienzentrum (IKMZ)

Das IKMZ ist an der BTU der Betreiber aller zentralen IT-Dienstleistungen. Es ist bei den von ihm betriebenen Systemen für die Sicherstellung eines angemessenen IT-Schutzes verantwortlich und wirkt als Impulsgeber bei der Fortschreibung des Informationssicherheitsprozesses.

Das Informationssicherheitsmanagement der BTU wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Prozesse und Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Angehörigen der BTU bekannt sind und ob sie umsetzbar und in den Universitätsablauf integrierbar sind.

Die Universitätsleitung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Alle Angehörigen der BTU sind angehalten, mögliche Verbesserungen oder Schwachstellen an den Informationssicherheitsbeauftragten weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und ständig auf dem aktuellen Stand der Informationssicherheitstechnik zu halten.

5. Geltungsbereich

Die Leitlinie für Informationssicherheit gilt für alle Einrichtungen der BTU, für alle IT-Systeme und Tätigkeiten, bei denen schutzbedürftige Informationen verarbeitet werden. Darüber hinaus gilt sie für die Gesamtheit der Nutzerinnen und Nutzer dieser Systeme. Hierzu zählen auch Beschäftigte beauftragter Dienstleistungsunternehmen, Kooperationspartner, An-Institute und Einrichtungen, die das Universitätsnetz oder dessen Netzinfrastruktur und IT-Dienste nutzen.

Der Anwendungsbereich des ISMS bezieht sich auf Bereitstellung und Betrieb von zentralen IT-

Services für Forschung, Lehre, Transfer und Verwaltung sowie angeschlossene externe Einrichtungen. Die Schnittstellen und Abhängigkeiten zum Anwendungsbereich sind in einer Richtlinie dokumentiert. Das CDO-Gremium ist ermächtigt, Richtlinien zur Informationssicherheit im Anwendungsbereich zu erlassen.

6. Inkrafttreten

Diese Informationssicherheitsleitlinie für die BTU tritt am Tag ihrer Veröffentlichung in den Amtlichen Mitteilungen der Universität in Kraft. Die vorliegende Informationssicherheitsleitlinie wurde von der Universitätsleitung am 11. April 2023 beschlossen.

Cottbus, 12. April 2023

gez. Prof. Dr. Gesine Grande
Präsidentin
der Brandenburgischen Technischen Universität
Cottbus-Senftenberg

[1] Informationen können Daten (z. B. Dokumente), Übertragungswege (z. B. E-Mail-Kommunikation oder Infrastruktur (z. B. Server) sein.

[2] https://bravors.brandenburg.de/gesetze/bbghg